IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Applicants: Brian Albert Wittman

Examiner: Vaughan, Michael R.

Serial No: 10/517,574

Group Art Unit: 2431

Filed: December 9, 2004

Docket: PU020277

For: DATA TRAFFIC FILTERING INDICATOR

Mail Stop Appeal Brief-Patents
Hon. Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPEAL BRIEF

Applicants appeal the status of Claims 1, 6-9, 16, and 18-35 as rejected in the final Office Action dated April 13, 2009 and the non-final Office Action dated February 2, 2009, pursuant to the Notice of Appeal filed concurrently herewith and submit this appeal brief

TABLE OF CONTENTS:

C2. Claim 31

C3. Claim 34

C4. Claim 22

D. Conclusion

8. CLAIMS APPENDIX

9. RELATED EVIDENCE APPENDIX

10. RELATING PROCEEDINGS APPENDIX

1. Real Party in Interest

The real party in interest is THOMSON LICENSING S.A., the assignee of the entire right title and interest in and to the subject application by virtue of an assignment recorded with the Patent Office on December 9, 2004 at reel/frame 016414/0084.

2. Related Appeals and Interferences

None

3. Status of Claims

Claims 1, 6-9, 16, and 18-35 are pending. Claims 1, 6-9, 16, and 18-35 stand rejected and are under appeal.

A copy of the Claims 1, 6-9, 16, and 18-35 is presented in Section 8 below.

4. Status of Amendments

An Amendment under 37 CFR §1.111, filed with the PTO on March 31, 2009 in response to a non-final Office Action dated February 2, 2009, was entered. No Responses/Amendments were filed subsequent to the above Amendment filed on March 31, 2009. A final Office Action dated April 13, 2009, to which this Appeal Brief is directed, is currently pending.

5. Summary of Claimed Subject Matter

Independent Claim 1 is directed to "[a]pparatus adapted to communicate via a network" (Claim 1, preamble).

The subject matter of the first element (beginning with "a firewall") recited in Claim 1 is described, e.g., at: page 4, lines 24-26; and page 10, lines 21-31. Moreover, the subject matter of the first element of Claim 1 involves, e.g.: element 124 of FIG. 1 and FIG. 2.

The subject matter of the second element (beginning with "an indicator device") recited in Claim 1 is described, e.g., at: page 4, lines 3-4; and page 12, lines 17-35. Moreover, the subject matter of the second element of Claim 1 involves, e.g.: element 126 of FIG. 1 and FIG. 2.

The subject matter of the third element (beginning with "wherein") recited in Claim 1 is described, e.g., at: page 10, lines 20-31. Moreover, the subject matter of the third element of Claim 1 involves, e.g.: element 124 of FIG. 1.

Independent Claim 7 is directed to "[a] method" (Claim 7, preamble).

The subject matter of the first element (beginning with "defining") recited in Claim 7 is described, e.g., at: page 4, line 34 to page 5, line 9. Moreover, the subject matter of the first element of Claim 7 involves, e.g.: element 124 of FIG. 1.

The subject matter of the second element (beginning with "separating") recited in Claim 7 is described, e.g., at: page 10, lines 20-31. Moreover, the subject matter of the second element of Claim 7 involves, e.g.: element 124 of FIG. 1.

The subject matter of the third element (beginning with "associating") recited in Claim 7 is described, e.g., at: page 12, lines 17-35. Moreover, the subject matter of the third element of Claim 7 involves, e.g.: 126 of FIG. 1.

The subject matter of the fourth element (beginning with "examining") recited in Claim 7 is described, e.g., at: page 10, lines 16-21. Moreover, the subject matter of the fourth element of Claim 7 involves, e.g.: element 124 of FIG. 1; and elements 302 and 304 of FIG. 3.

The subject matter of the fifth element (beginning with "in the case") recited in Claim 7 is described, e.g., at: page 10, lines 20-31; and page 12, lines 17-35. Moreover, the subject matter of the fifth element of Claim 7 involves, e.g.: elements 124 and 126 of FIG. 1; and elements 318 and 320 of FIG. 3.

Independent Claim 16 is directed to "[a] cable modem" (Claim 16, preamble).

The subject matter of the first element (beginning with "downstream processing circuitry") recited in Claim 16 is described, e.g., at: page 7, lines 27-33. Moreover, the subject matter of the first element of Claim 16 involves, e.g.: element 210 of FIG. 2.

The subject matter of the second element (beginning with "upstream processing circuitry") recited in Claim 16 is described, e.g., at: page 8, lines 17-20. Moreover, the subject matter of the second element of Claim 16 involves, e.g.: element 212 of FIG. 2.

The subject matter of the third element (beginning with "a controller") recited in Claim 16 is described, e.g., at: page 4, lines 5-8; and page 7, lines 31-33. Moreover, the subject matter of the third element of Claim 16 involves, e.g.: element 104 of FIG. 1; and element 204 of FIG. 2.

The subject matter of the fourth element (beginning with "a firewall program") recited in Claim 16 is described, e.g., at: page 4, lines 24-26; page 9, lines 3-5 and 24-26; and page 10, lines 21-31. Moreover, the subject matter of the fourth element of Claim 16 involves, e.g.: element 124 of FIG. 1 and FIG. 2.

The subject matter of the fifth element (beginning with "a plurality of user discernable indicators") recited in Claim 16 is described, e.g., at: page 4, lines 3-4; and page 12, lines 17-35. Moreover, the subject matter of the fifth element of Claim 16 involves, e.g.: element 126 of FIG. 1 and FIG. 2.

6. Grounds of Rejection to be Reviewed on Appeal

Claims 25, 29, and 33 stand rejected under 35 U.S.C. 112, second paragraph. The preceding rejection under 35 U.S.C. 112, second paragraph is NOT currently being appealed, and will be addressed subsequent to a decision on the appeal.

Claims 1, 6-9, 20, 21, 23-30, and 35 stand rejected under 35 U.S.C. §103(a) as being unpatentable over ZoneAlarm publication by Ash Nallawalla (hereinafter "ZoneAlarm") in view of U.S. Patent Publication No. 2002/0178383 to Hrabik et al. (hereinafter "Hrabik"). Moreover, Claims 16, 18, 19, 22, and 31-34 stand rejected under as being unpatentable over ZoneAlarm in view of Hrabik and in view of U.S. Patent No. 6,185,624B1 to Fijolek et al. (hereinafter "Fijolek").

The preceding rejections under 35 U.S.C. 103(a) are presented for review in this Appeal.

Regarding the grouping of the claims, Claims 6, 20, 23-26, and 35 stand or fall with Claim 1 due to their respective dependencies, Claims 8, 9, 21, and 27-30 stand or fall with Claim 7 due to their respective dependencies, and Claims 18, 19, 22, and 31-34 stand or fall with Claim 16 due to their respective dependencies.

7. Argument

A. Introduction

In general, the present invention is directed to a data traffic filtering indicator (Applicant's Specification, Title). As disclosed in the Applicant's specification at page 1, line 33 to page 2, line 7:

> Typical software-based firewall programs log events in a log file. The firewall programs do not provide contemporaneous feedback when, for example, a hacker is trying to infiltrate the network. Rather, a dialog window may subsequently be provided when a filtering event occurs. The dialog windows require user action to clear the screen. Repeated filtering by the firewall program repetitiously initiates the dialog window and requires constant user interaction to clear the screen, which may become annoying to the user. Many users simply disable the dialog window, and only keep the logging to the log file enabled. As such, there is a need to notify a system administrator or end-user of instances where data traffic is being blocked (i.e., filtered) by a firewall program in a network environment.

The claims of the pending invention include novel features not shown in the cited references and that have already been pointed out to the Examiner. These features provide advantages over the prior art and dispense with prior art problems such as those described above with reference to the Applicant's specification.

It is respectfully asserted that independent Claims 1, 7, and 16 are each patentably distinct and non-obvious over the cited references in their own right. For example, the below-identified limitations of independent Claims 1, 7, and 16 are not shown in any of the cited references, either taken singly or in any combination. Moreover, these Claims are distinct from each other in that they are directed to different implementations and/or include different limitations. For example,

Claim 1 is directed to an apparatus, while Claim 7 is directed to a method, and Claim 16 is directed to a cable modem. Moreover, each of these claims includes different limitations with respect to each other. Accordingly, each of independent Claims 1, 7, and 16 represent separate features/implementations of the invention that are separately novel and non-obvious with respect to the prior art and to the other claims. As such, independent Claims 1, 7, and 16 are separately patentable and are each presented for review in this appeal.

B. Whether Claims 1, 6-9, 20, 21, 23-30, and 35 are Unpatentable Under 35 U.S.C. §103(a) With Respect To ZoneAlarm Publication by Ash Nallawalla in view of U.S. Patent App. Pub. No. 2002/0178383 to Hrabik et al.

"To establish prima facie obviousness of a claimed invention, all the claim limitations must be taught or suggested by the prior art" (MPEP §2143.03, citing *In re Royka*, 490 F.2d 981, 180 USPQ 580 (CCPA 1974)). "If an independent claim is nonobvious under 35 U.S.C. 103, then any claim depending therefrom is nonobvious" (MPEP §2143.03, citing *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988)).

The Examiner rejected Claims 1, 6-9, 20, 21, 23-30, and 35 as being unpatentable over ZoneAlarm Publication by Ash Nallawalla (hereinafter "ZoneAlarm") in view of U.S. Patent App. Pub. No. 2002/0178383 to Hrabik et al. (hereinafter "Hrabik"). The Examiner contends that the cited combination shows all the limitations recited in Claims 1, 6-9, 20, 21, 23-30, and 35.

ZoneAlarm is directed to "ZoneAlarm Pro 3.0" (ZoneAlarm, Title). In further detail, ZoneAlarm discloses the following:

ZA Pro looks quite different from ZA so it takes a while to get reacquainted with the features it shares with ZA.

Like its junior cousin, ZA Pro gives you the option of Installing with conservative settings that will protect you.

What's Extra? Here are the extra features in ZA Pro compared with ZA:

- It can block advertisements and popups.
- It can block 46 types of potentially nasty file attachments that can come with e-mail, compared to one type blocked by ZA. .
- It can block active content found on some Web sites.
- It can block cookies.
- You can find the approximate geographical16cation of a cracker who is probing you (a "hacker" is what ignorant people call a "cracker").
- You can block specific IP addresses if they are known to be pests.
- Laptop computers can adapt easily to a new network, such as using it at home, work, and at a branch office.
- You can protect your ZA pro settings with a password.

Hrabik is directed to a "method and apparatus for verifying the integrity and security of computer networks and implementing counter measure" (Hrabik, Title). In further detail, Hrabik discloses the following in his Abstract:

A method and apparatus for verifying the integrity of devices on a target network. The apparatus has security subsystems and a master security system hierarchically connected to the security subsystems via a secure link. The target network includes various intrusion detection devices, which may be part of the

security subsystem. Each intrusion detection device generates a plurality of event messages when an attack on the network is detected. The security subsystem collects these event messages, correlates, and analyzes them, and performs network scanning processes. If certain events warrant additional scrutiny, they are uploaded to the master security system for review.

It will be shown herein below that the limitations of Claims 1, 6-9, 20, 21, 23-30, and 35 reproduced herein (as argued with respect to independent claims from which they respectively depend) are not shown in the cited combination, and that Claims 1, 6-9, 20, 21, 23-30, and 35 should be allowed.

B1. Claims 1, 6-9, 20, 21, 23-30, and 35

Initially, it is respectfully pointed out to the Examiner that Claims 6, 20, 23-26, and 35 directly or indirectly depend from independent Claim 1. Thus, Claims 6, 20, 23-26, and 35 include all the limitations of Claim 1.

Moreover, it is respectfully pointed out to the Examiner that Claims 8, 9, 21, and 27-30 directly or indirectly depend from independent Claim 7. Thus, Claims 8, 9, 21, and 27-30 include all the limitations of Claim 7.

It is respectfully asserted that none of the cited references, either taken singly or in combination, teach or suggest the following limitations of Claims 1, 6, 20, 23-26, and 35 (with the following applicable to Claims 6, 20, 23-26, and 35 by virtue of their respective dependencies from Claim 1): "the rules in the set being separated into a plurality of classes".

Moreover, it is respectfully asserted that none of the cited references, either taken singly or in combination, teach or suggest the following limitations of Claims 7, 8, 9, 21, and 27-30 (with the following applicable to Claims 8, 9, 21, 27, and 30 by virtue of their respective dependencies from Claim 7): "separating the rules in the set into a plurality of classes".

Against the preceding limitations of Claim 1 (and, hence, also, Claims 6, 20, 23-26, and 35), the Examiner has simply cited "ZoneAlarm alerts" (see, Office Action, p. 8). Against the preceding limitations of Claim 7 (and, hence, also Claims 8, 9, 21, 27, and 30), the Examiner has simply cited "classes are outgoing traffic, incoming traffic, identifying/privacy data, and malicious code" (see, Office Action, p. 10).

However, the above cited reference ZoneAlarm by Ash Nallawalla does not include even one single occurrence of the words "class" or "classes" as recited in the pending claims, let alone, "outgoing traffic", "incoming traffic", "identifying/privacy data", and "malicious code" as alleged by the Examiner as being disclosed therein. As the Examiner has explicitly stated "First of all, ZoneAlarm teaches rules and classes" (Office Action, p. 5), the Applicants respectfully disagree with the Examiner's reading of ZoneAlarm.

It is respectfully asserted that Hrabik does not cure the deficiencies of ZoneAlarm, and is silent with respect to the above recited limitations of the pending claims.

Hence, for at least the preceding reasons, both ZoneAlarm and/or Hrabik, either taken singly or in combination, fail to teach or suggest the preceding recited limitations of the pending claims.

Additionally, it is respectfully asserted that none of the cited references, either taken singly or in combination, teach or suggest the following limitations of Claims 1, 6-9, 20, 21, 23-

30, and 35 (with the following applicable to Claims 6, 20, 23-26, and 35 by virtue of their respective dependencies from Claim 1, and to Claims 8, 9, 21, and 27-30 by virtue of their respective dependencies from Claim 7): "wherein the rules in the set are prioritized such that each of the plurality of classes represents a respective different one of a plurality of priority levels".

In fact, the Examiner has explicitly admitted on page 9 of the Office Action dated April 13, 2009 that "ZoneAlarm is silent in explicitly disclosing the rules in the set are prioritized such that each of the plurality of classes represents a respective different one of a plurality of priority levels".

Hence, the Examiner has cited paragraph [0060] of Hrabik as disclosing the same, reasoning "In an effort to only interrupt a system administer with the utmost critical alerts, Hrabik teaches a firewall system in which the threats are prioritized and put into classes whereby only the higher classes are immediately sent to a system engineer for responsive actions". The Applicants respectfully disagree with the Examiner's reading of Hrabik.

The only seemingly relevant part of paragraph [0060] of Hrabik with respect to the above limitations is as follows:

> The target network can be divided into a plurality of security zones. Different security zones might differ in their importance to the company and, thus, have a different level of security risk. Accordingly, each uploaded security event may be further classified by its level of security risk in accordance with the security zone where it was last detected.

Claims 1, 6-9, 20, 21, 23-30, and 35 involve and explicitly recite, *inter alia*, rules,

classes, and priority levels. In further detail, Claims 1, 6-9, 20, 21, 23-30, and 35 essentially recite that the rules in a set of rules (included in a firewall) are separated into a plurality of classes and prioritized such that each of the plurality of classes represents a respective different one of a plurality of priority levels. The cited portion of Hrabik makes no explicit mention of rules, or classes, or priority levels. All that is disclosed in paragraph [0060] of Hrabik is that each uploaded security event may be further classified by its level of security risk in accordance with the security zone where it was last detected. Hence, **in Hrabik, the actual event itself is being classified based on which security zone the event was last detected. Thus, contrary to the rules in the set being separated into a plurality of classes (and hence classified), Hrabik directly classifies the actual event itself.** That is, in the case of Hrabik, the classification (and, hence, class) of the actual event is the security risk (priority level), without regard to any underlying rule. **Prioritizing a rule as explicitly claimed in Claims 1, 6-9, 20, 21, 23-30, and 35 does not correspond to prioritizing an actual event itself. For example, a rule is what is compared against an actual event to determine whether the rule is violated by the event in the first place.** Hence, there is, for lack of a better term, a layer (and thus, certainly at least one claimed element) missing in the approach of Hrabik, as essentially admitted by the Examiner. That is, while Claims 1, 6-9, 20, 21, 23-30, and 35 recite, *inter alia*, separating rules in a set into a plurality of classes and prioritizing the rules such that each of the classes represents a respective different priority level, in contrast **as admitted by the Examiner Hrabik discloses "the threats are prioritized and put into classes"** (Office Action, dated February 2, 2009, p. 6). For example, even the Examiner noted the preceding distinction in the Office Action, as follows;

> **ZoneAlarm is silent** in explicitly disclosing ***the rules in the set are prioritized such that each of the plurality of classes represents a respective different one of a plurality of priority levels***. In an effort to only interrupt a system administrator with the utmost critical alerts, *Hrabik* teaches a firewall system in which *the threats are prioritized and put into classes* whereby only the higher classes are immediately sent to a system engineer for responsive actions (0060). Hrabik classifies threads but [sic-based] the security risk to the network.

Hence, based on the preceding, neither ZoneAlarm nor Hrabik teach or suggest "wherein the rules in the set are prioritized such that each of the plurality of classes represents a respective different one of a plurality of priority levels", as recited in Claims 1, 6-9, 20, 21, 23-30, and 35.

Thus, it is respectfully asserted that the cited combination of ZoneAlarm and Hrabik does not teach or suggest the above recited limitations of Claims 1, 6-9, 20, 21, 23-30, and 35. Moreover, the remaining reference does not cure the deficiencies of ZoneAlarm and/or Hrabik, and is silent with respect to the above recited limitations of Claims 1, 6-9, 20, 21, 23-30, and 35.

Accordingly, Claims 1, 6-9, 20, 21, 23-30, and 35 are patentably distinct and non-obvious over the cited references for at least the reasons set forth above. Therefore, withdrawal of the rejection and allowance of Claims 1, 6-9, 20, 21, 23-30, and 35 is earnestly requested.

B2. Claims 23 and 27

It is respectfully asserted that none of the cited references, either taken singly or in combination, teach or suggest the following limitations of Claim 23:

wherein each of the plurality of user discernable indicators except a particular one is associated with the respective different one of the plurality of classes, the particular one of the plurality of user discernable indicators being associated with an affirmative status that filtering is being contemporaneously performed for any of the packets that violate the one or more rules, and wherein the method further comprises filtering any of the packets that violate the one or more rules, and wherein the particular one of the plurality of user discernable indicators is concurrently triggered, along with the respective one of the plurality of user discernable indicators, to indicate that the filtering is being contemporaneously performed, only when a number of the packets that violate the one or more rules exceeds a pre-specified threshold.

Moreover, it is respectfully asserted that none of the cited references, either taken singly or in combination, teach or suggest the following limitations of Claim 27:

wherein each of the plurality of user discernable indicators except a particular one is associated with the different one of the plurality of classes, and the method further comprises:

associating the particular one of the plurality of user discernable indicators with an affirmative status that filtering is being contemporaneously performed for any of the packets that violate at least one of the rules; and

in the case of the rule of at least a first class from among the plurality of classes being violated and a number of packets violating the rule of at least the first class exceeding a pre-specified threshold, providing a user discernable notification of the filtering being contemporaneously performed by triggering, concurrently with the triggering of the respective one of the plurality of user discernable indicators, the particular one of the plurality of user discernable indicators associated with the affirmative status that the filtering is being contemporaneously performed.

Against the preceding limitations of Claims 23 and 27, and particularly with respect to the particular one (indicator) recited therein, the Examiner has cited a system tray icon allegedly from ZoneAlarm. **First, the Applicants respectfully point out that while the Examiner has reproduced a description of system tray icons on page 19 of the Office Action, such reproduction from the Office Action is NOT found in the cited ZoneAlarm reference.**

Nonetheless, this reproduction will now be addressed. Five icons are shown on page 19 of the Office Action, with the third from the top being explicitly identified by the Examiner on page 19 as showing filtering, which would arguably relate to the recited particular one (indicator). However, the third icon from the top is described as "Zone Labs security software has blocked a communication, but your setting prevent a full-sized alert from being shown". Thus, it is clear from the description of this icon that only this icon may be seen, as this particular icon is associated with a setting that uses this icon IN PLACE OF all full-size (i.e., OTHER) alerts. Hence, while Claims 23 and 27 recite, *inter alia*, the concurrent triggering of two user discernable indicators, namely the particular one (indicator) and the respective one (indicator), the third icon from the top cited by the Examiner on page 19 of the Office Action can only be used by itself (i.e., without any full-size (i.e., other) indicators). Thus, the third icon cannot correspond to the particular one (indicator) recited in Claims 23 and 27, as the particular one (indicator) is able to be triggered concurrently with the respective one (indicator).

Hence, for at least the preceding reasons, ZoneAlarm fails to teach or suggest the above recited limitations of Claims 23 and 27. Moreover, the remaining references do not cure the

deficiencies of ZoneAlarm, and are silent with respect to the above recited limitations of Claims 23 and 27.

Accordingly, Claims 23 and 27 are patentably distinct and non-obvious over the cited references for at least the reasons set forth above. Therefore, withdrawal of the rejection and allowance of Claims 23 and 27 is earnestly requested.

B3. Claims 26 and 30

It is respectfully asserted that none of the cited references, either taken singly or in combination, teach or suggest the following limitations of Claim 26: "wherein whether the respective one of the plurality of user discernable indicators is triggered or not is based on which of the plurality of priority levels is involved with respect to a corresponding rule violation."

Moreover, it is respectfully asserted that none of the cited references, either taken singly or in combination, teach or suggest the following limitations of Claim 30: "wherein whether the respective one of the plurality of user discernable indicators is triggered or not is based on which of the plurality of priority levels is involved with respect to a corresponding rule violation."

Against the preceding limitations of Claims 26 and 30, the Examiner has cited paragraph [0060] of Hrabik, reasoning "Hrabik teaches the priority levels of the threat determine the countermeasure (0060)".

Paragraph 0060 of Hrabik simply discloses, *inter alia*,: "The master system 60 may also utilize risk threshold criteria against which all uploaded security events are compared. When an uploaded event exceeds a risk threshold, automatic countermeasures may be implemented."

However, paragraph [0060] of Hrabik is completely silent with respect to user discernable

indicators, and a countermeasure is a measure taken to fix the threat and not necessarily to alert a user to the same. Hence, for at least the preceding reasons, ZoneAlarm and/or Hrabik fail to teach or suggest the above recited limitations of Claims 26 and 30. Moreover, the remaining reference does not cure the deficiencies of ZoneAlarm, and is silent with respect to the above recited limitations of Claims 26 and 30.

Accordingly, Claims 26 and 30 are patentably distinct and non-obvious over the cited references for at least the reasons set forth above. Therefore, withdrawal of the rejection and allowance of Claims 26 and 30 is earnestly requested.

B4. Claims 20 and 21

It is respectfully asserted that none of the cited references, either taken singly or in combination, teach or suggest the following limitations of Claim 20:

> wherein the firewall filters any of the packets that violate the one or more rules irrespective of a number of the packets that violate the one or more rules, but only triggers the respective one of the plurality of user discernable indicators when the number of the packets that violate the one or more rules exceeds a pre-specified threshold.

Moreover, it is respectfully asserted that none of the cited references, either taken singly or in combination, teach or suggest the following limitations of Claim 21:

> wherein the data traffic includes a number of packets that violate the at least one of the rules of the first one of the plurality of classes, and wherein the method

filters the packets that violate the at least one of the rules of the first one of the plurality of classes, irrespective of the number of packets that violate the one or more rules, but only triggers the respective one of the plurality of user discernable indicators when the number of packets that violate the at least one of the rules of the first one of the plurality of classes exceeds a pre-specified threshold.

Against the preceding limitations of Claims 20 and 21, the Examiner has cited paragraphs [0059]-[0060] of Hrabik, reasoning "ZoneAlarm is silent in disclosing determining if a first threshold level of rule violation has been exceeded prior to triggering the user discernable indicator. Hrabik teaches determining if a first threshold level of rule violation has been exceeded prior to triggering the user discernable indicator (0059, 0060)." The Applicants respectfully disagree. Paragraph 0059 of Hrabik simply discloses: "A network event analyzer analyzes data in various views, described above, looking for events exceeding predetermined thresholds." Paragraph 0060 of Hrabik simply discloses: "The master system 60 may also utilize risk threshold criteria against which all uploaded security events are compared. When an uploaded event exceeds a risk threshold, automatic countermeasures may be implemented." However, none of the preceding cited portions of Hrabik even remotely disclose premising whether a user discernable indication is provided based on a threshold as recited.

Hence, for at least the preceding reasons, ZoneAlarm and/or Hrabik fail to teach or suggest the above recited limitations of Claims 20 and 21. Moreover, the remaining reference does not cure the deficiencies of ZoneAlarm, and is silent with respect to the above recited limitations of Claims 20 and 21.

Accordingly, Claims 20 and 21 are patentably distinct and non-obvious over the cited

references for at least the reasons set forth above. Therefore, withdrawal of the rejection and allowance of Claims 20 and 21 is earnestly requested.

C. Whether Claims 16, 18, 19, 22, and 31-34 are Unpatentable Under 35 U.S.C. §103(a) With Respect To ZoneAlarm Publication by Ash Nallawalla in view of U.S. Patent App. Pub. No. 2002/0178383 to Hrabik et al. and in view of U.S. Patent No. 6,185,624 to Fijolek et al.

"To establish prima facie obviousness of a claimed invention, all the claim limitations must be taught or suggested by the prior art" (MPEP §2143.03, citing *In re Royka*, 490 F.2d 981, 180 USPQ 580 (CCPA 1974)). "If an independent claim is nonobvious under 35 U.S.C. 103, then any claim depending therefrom is nonobvious" (MPEP §2143.03, citing *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988)).

The Examiner rejected Claims 16, 18, 19, 22, and 31-34 as being unpatentable over ZoneAlarm Publication by Ash Nallawalla (hereinafter "ZoneAlarm") in view of U.S. Patent App. Pub. No. 2002/0178383 to Hrabik et al. (hereinafter "Hrabik") in view of U.S. Patent No. 6,185,624 to Fijolek et al. The Examiner contends that the cited combination shows all the limitations recited in Claims 16, 18, 19, 22, and 31-34.

ZoneAlarm is directed to "ZoneAlarm Pro 3.0" (ZoneAlarm, Title). In further detail, ZoneAlarm discloses the following:

> ZA Pro looks quite different from ZA so it takes a while to get reacquainted with the features it shares with ZA.
> Like its junior cousin, ZA Pro gives you the option of Installing with conservative

settings that will protect you.

What's Extra? Here are the extra features in ZA Pro compared with ZA:

- It can block advertisements and popups.
- It can block 46 types of potentially nasty file attachments that can come with e-mail, compared to one type blocked by ZA. .
- It can block active content found on some Web sites.
- It can block cookies.
- You can find the approximate geographical16cation of a cracker who is probing you (a "hacker" is what ignorant people call a "cracker").
- You can block specific IP addresses if they are known to be pests.
- Laptop computers can adapt easily to a new network, such as using it at home, work, and at a branch office.
- You can protect your ZA pro settings with a password.

Hrabik is directed to a "method and apparatus for verifying the integrity and security of computer networks and implementing counter measure" (Hrabik, Title). In further detail, Hrabik discloses the following in his Abstract:

> A method and apparatus for verifying the integrity of devices on a target network. The apparatus has security subsystems and a master security system hierarchically connected to the security subsystems via a secure link. The target network includes various intrusion detection devices, which may be part of the security subsystem. Each intrusion detection device generates a plurality of event messages when an attack on the network is detected. The security subsystem collects these event messages, correlates, and analyzes them, and performs network scanning processes. If certain events warrant additional scrutiny, they are uploaded to the master security system for review.

Fijolek is directed to a "method and system for cable modem management of a data-over-cable system" (Fijolek, Title). In further detail, Fijolek discloses the following in his Abstract:

> A method and system for providing management functionality with a cable modem with telephony return is provided. The cable modem with telephony return is used for providing management functionality such as maintenance and signaling via the lower bandwidth telephony return path, leaving more higher bandwidth cable television channels free for data transmission. Since routine management functions such as maintenance are completed on the cable television channels via the telephony return path, the overall costs of maintaining the higher bandwidth cable television channels are reduced. In addition, since routine management functions are carried out via the telephony return path, fewer overall maintenance functions need to be carried out on the higher bandwidth cable television channels, requiring less down time and generating more revenues for the cable television network providers.

It will be shown herein below that the limitations of Claims 16, 18, 19, 22, and 31-34 reproduced herein (as argued with respect to independent claims from which they respectively depend) are not shown in the cited combination, and that Claims 16, 18, 19, 22, and 31-34 should be allowed.

C1. Claims 16, 18, 19, 22, and 31-34

Initially, it is respectfully pointed out to the Examiner that Claims 18, 19, 22, 31, and 34 directly or indirectly depend from independent Claim 16. Thus, Claims 18, 19, 22, 31, and 34 include all the limitations of Claim 16.

It is respectfully asserted that none of the cited references, either taken singly or in combination, teach or suggest the following limitations of Claims 16, 18, 19, 22, 31, and 34 (with the following applicable to Claims 18, 19, 22, 31, and 34 by virtue of their respective dependencies from Claim 16): "the rules being separated into a plurality of classes".

Against the preceding limitations of Claim 16 (and, hence, also Claims 18, 19, 22, 31, and 34), the Examiner has simply cited "classes are outgoing traffic, incoming traffic, identifying/privacy data, and malicious code" (see, Office Action, p. 17).

However, the above cited reference ZoneAlarm by Ash Nallawalla does not include even one single occurrence of the words "class" or "classes" as recited in the pending claims, let alone, "outgoing traffic", "incoming traffic", "identifying/privacy data", and "malicious code" as alleged by the Examiner as being disclosed therein. As the Examiner has explicitly stated "First of all, ZoneAlarm teaches rules and classes" (Office Action, p. 5), the Applicants respectfully disagree with the Examiner's reading of ZoneAlarm.

It is respectfully asserted that neither Hrabik nor Fijolek cure the deficiencies of ZoneAlarm, and are silent with respect to the above recited limitations of the pending claims.

Hence, for at least the preceding reasons, ZoneAlarm and/or Hrabik and/or Fijolek, either taken singly or in combination, fail to teach or suggest the preceding recited limitations of the pending claims.

Additionally, it is respectfully asserted that none of the cited references, either taken singly or in combination, teach or suggest the following limitations of Claims 16, 18, 19, 22, 31, and 34 (with the following applicable to Claims 18, 19, 22, 31, and 34 by virtue of their respective dependencies from Claim 16): "wherein the rules in the set are prioritized such that each of the plurality of classes represents a respective different one of a plurality of priority levels".

In fact, the Examiner has explicitly admitted on page 9 of the Office Action dated April 13, 2009 that "ZoneAlarm is silent in explicitly disclosing the rules in the set are prioritized such that each of the plurality of classes represents a respective different one of a plurality of priority levels".

Hence, the Examiner has cited paragraph [0060] of Hrabik as disclosing the same, reasoning "In an effort to only interrupt a system administer with the utmost critical alerts, Hrabik teaches a firewall system in which the threats are prioritized and put into classes whereby only the higher classes are immediately sent to a system engineer for responsive actions". The Applicants respectfully disagree with the Examiner's reading of Hrabik.

The only seemingly relevant part of paragraph [0060] of Hrabik with respect to the above limitations is as follows:

> The target network can be divided into a plurality of security zones. Different security zones might differ in their importance to the company and, thus, have a different level of security risk. Accordingly, each uploaded security event may be further classified by its level of security risk in accordance with the security zone where it was last detected.

Claims 16, 18, 19, 22, 31, and 34 involve and explicitly recite, *inter alia*, rules, classes, and priority levels. In further detail, Claims 16, 18, 19, 22, 31, and 34 essentially recite that the rules in a set of rules (included in a firewall) are separated into a plurality of classes and prioritized such that each of the plurality of classes represents a respective different one of a plurality of priority levels. The cited portion of Hrabik makes no explicit mention of rules, or classes, or priority levels. All that is disclosed in paragraph [0060] of Hrabik is that each uploaded security event may be further classified by its level of security risk in accordance with the security zone where it was last detected. Hence, **in Hrabik, the actual event itself is being classified based on which security zone the event was last detected. Thus, contrary to the rules in the set being separated into a plurality of classes (and hence classified), Hrabik directly classifies the actual event itself.** That is, in the case of Hrabik, the classification (and, hence, class) of the actual event is the security risk (priority level), without regard to any underlying rule. **Prioritizing a rule as explicitly claimed in Claims 16, 18, 19, 22, 31, and 34 does not correspond to prioritizing an actual event itself. For example, a rule is what is compared against an actual event to determine whether the rule is violated by the event in the first place.** Hence, there is, for lack of a better term, a layer (and thus, certainly at least one claimed element) missing in the approach of Hrabik, as essentially admitted by the Examiner. That is, while Claims 16, 18, 19, 22, 31, and 34 recite, *inter alia*, separating rules in a set into a plurality of classes and prioritizing the rules such that each of the classes represents a respective different priority level, in contrast **as admitted by the Examiner Hrabik discloses "the threats are prioritized and put into classes"** (Office Action, dated February 2, 2009, p. 6). For example, even the Examiner noted the preceding distinction in the Office Action, as follows;

> **ZoneAlarm is silent** in explicitly disclosing ***the rules in the set are prioritized such that each of the plurality of classes represents a respective different one of a plurality of priority levels***. In an effort to only interrupt a system administrator with the utmost critical alerts, *Hrabik* teaches a firewall system in which *the threats are prioritized and put into classes* whereby only the higher classes are immediately sent to a system engineer for responsive actions (0060). Hrabik classifies threads but [sic-based] the security risk to the network.

Hence, based on the preceding, neither ZoneAlarm nor Hrabik teach or suggest "wherein the rules in the set are prioritized such that each of the plurality of classes represents a respective different one of a plurality of priority levels", as recited in Claims 16, 18, 19, 22, 31, and 34.

Thus, it is respectfully asserted that the cited combination of ZoneAlarm and Hrabik does not teach or suggest the above recited limitations of Claims 16, 18, 19, 22, 31, and 34. Moreover, the remaining reference does not cure the deficiencies of ZoneAlarm and/or Hrabik, and is silent with respect to the above recited limitations of Claims 16, 18, 19, 22, 31, and 34.

Accordingly, Claims 16, 18, 19, 22, 31, and 34 are patentably distinct and non-obvious over the cited references for at least the reasons set forth above. Therefore, withdrawal of the rejection and allowance of Claims 16, 18, 19, 22, 31, and 34 is earnestly requested.

C2. Claim 31

It is respectfully asserted that none of the cited references, either taken singly or in combination, teach or suggest the following limitations of Claim 31:

wherein the firewall program is executable by said controller to cause filtering any of the packets that at least one of the rules, and wherein each of the plurality of user discernable indicators other than a particular one is respectively associated with the different ones of the plurality of classes, the particular one of the plurality of user discernable indicators being associated with an affirmative status that filtering is being contemporaneously performed, and wherein the particular one of the plurality of user discernable indicators is triggered, concurrently with the triggering of the respective one of the plurality of user discernable indicators, if the one or more of the rules is violated, the filtering is performed by the firewall program, and a number of the packets that violate the one or more rules exceeds a pre-specified threshold.

Against the preceding limitations of Claim 31, and particularly with respect to the particular one (indicator) recited therein, the Examiner has cited a system tray icon allegedly from ZoneAlarm. **First, the Applicants respectfully point out that while the Examiner has reproduced a description of system tray icons on page 19 of the Office Action, such reproduction from the Office Action is NOT found in the cited ZoneAlarm reference.**

Nonetheless, this reproduction will now be addressed. Five icons are shown on page 19 of the Office Action, with the third from the top being explicitly identified by the Examiner on page 19 as showing filtering, which would arguably relate to the recited particular one (indicator). However, the third icon from the top is described as "Zone Labs security software has blocked a communication, but your setting prevent a full-sized alert from being shown". Thus, it is clear from the description of this icon that only this icon may be seen, as this particular icon is associated with a setting that uses this icon IN PLACE OF all full-size (i.e., OTHER) alerts. Hence, while Claim 31 recites, *inter alia*, the concurrent triggering of two user

discernable indicators, namely the particular one (indicator) and the respective one (indicator), the third icon from the top cited by the Examiner on page 19 of the Office Action can only be used by itself (i.e., without any full-size (i.e., other) indicators). Thus, the third icon cannot correspond to the particular one (indicator) recited in Claim 31, as the particular one (indicator) is able to be triggered concurrently with the respective one (indicator).

Hence, for at least the preceding reasons, ZoneAlarm fails to teach or suggest the above recited limitations of Claim 31. Moreover, the remaining references do not cure the deficiencies of ZoneAlarm, and are silent with respect to the above recited limitations of Claim 31.

Accordingly, Claim 31 is patentably distinct and non-obvious over the cited references for at least the reasons set forth above. Therefore, withdrawal of the rejection and allowance of Claim 31 is earnestly requested.

C3. Claim 34

It is respectfully asserted that none of the cited references, either taken singly or in combination, teach or suggest the following limitations of Claim 34: "wherein whether the respective one of the plurality of user discernable indicators is triggered or not is based on which of the plurality of priority levels is involved with respect to a corresponding rule violation."

Against the preceding limitations of Claim 34, the Examiner has cited paragraph [0060] of Hrabik, reasoning "Hrabik teaches the priority levels of the threat determine the countermeasure (0060)".

Paragraph 0060 of Hrabik simply discloses, *inter alia*,: "The master system 60 may also utilize risk threshold criteria against which all uploaded security events are compared. When an

uploaded event exceeds a risk threshold, automatic countermeasures may be implemented." **However, paragraph [0060] of Hrabik is completely silent with respect to user discernable indicators, and a countermeasure is a measure taken to fix the threat and not necessarily to alert a user to the same.** Hence, for at least the preceding reasons, ZoneAlarm and/or Hrabik fail to teach or suggest the above recited limitations of Claim 34. Moreover, the remaining reference does not cure the deficiencies of ZoneAlarm, and is silent with respect to the above recited limitations of Claim 34.

Accordingly, Claim 34 is patentably distinct and non-obvious over the cited references for at least the reasons set forth above. Therefore, withdrawal of the rejection and allowance of Claim 34 is earnestly requested.

C4. Claim 22

It is respectfully asserted that none of the cited references, either taken singly or in combination, teach or suggest the following limitations of Claim 22:

> wherein the firewall program is executable by said controller to cause filtering of any of the packets that violate the one or more rules irrespective of a number of the packets that violate the one or more rules, but wherein the respective one of the plurality of user discernable indicators is triggered only when the number of packets that violate the one or more rules exceeds a pre-specified threshold.

Against the preceding limitations of Claim 22, the Examiner has cited paragraphs [0059]-[0060] of Hrabik, reasoning "ZoneAlarm is silent in disclosing determining if a first threshold

level of rule violation has been exceeded prior to triggering the user discernable indicator. Hrabik teaches determining if a first threshold level of rule violation has been exceeded prior to triggering the user discernable indicator (0059, 0060)." The Applicants respectfully disagree. Paragraph 0059 of Hrabik simply discloses: "A network event analyzer analyzes data in various views, described above, looking for events exceeding predetermined thresholds." Paragraph 0060 of Hrabik simply discloses: "The master system 60 may also utilize risk threshold criteria against which all uploaded security events are compared. When an uploaded event exceeds a risk threshold, automatic countermeasures may be implemented." However, none of the preceding cited portions of Hrabik even remotely disclose premising whether a user discernable indication is provided based on a threshold as recited.

Hence, for at least the preceding reasons, ZoneAlarm and/or Hrabik fail to teach or suggest the above recited limitations of Claim 22. Moreover, the remaining reference does not cure the deficiencies of ZoneAlarm, and is silent with respect to the above recited limitations of Claim 22.

Accordingly, Claim 22 is patentably distinct and non-obvious over the cited references for at least the reasons set forth above. Therefore, withdrawal of the rejection and allowance of Claim 22 is earnestly requested.

D. Conclusion

At least the above-identified limitations of the pending claims are not disclosed or suggested by the teachings of the cited references. Accordingly, it is respectfully requested that the Board reverse the rejections of Claim 1, 6-9, 16, and 18-35 under 35 U.S.C. §103(a).

Please charge the amount of $540.00, covering fee associated with the filing of the Appeal Brief, to **Thomson Licensing Inc., Deposit Account No. 07-0832**. In the event of any non-payment or improper payment of a required fee, the Commissioner is authorized to charge **Deposit Account No. 07-0832** as required to correct the error.

Respectfully submitted,

BY: /Guy Eriksen/
Guy Eriksen, Attorney for Applicant
Registration No.: 41,736
Telephone No.: (609) 734-6807

Thomson Licensing LLC
Patent Operations
P.O. Box 5312
Princeton, NJ 08543-5312

June 25, 2009

8. CLAIMS APPENDIX

1. (previously presented) Apparatus adapted to communicate via a network, comprising:

a firewall including a set of rules for identifying packets associated with inappropriate activity, the rules in the set being separated into a plurality of classes; and

an indicator device for providing a plurality of user discernable indicators, wherein each of the plurality of user discernable indicators is associated with a different one of the plurality of classes, and wherein a respective one of said plurality of user discernable indicators is triggered if one or more of the rules corresponding to one of said plurality of classes associated with the respective one of said plurality of user discernable indicators is violated,

wherein the rules in the set are prioritized such that each of the plurality of classes represents a respective different one of a plurality of priority levels.

2-5. (cancelled)

6. (previously presented) The apparatus of claim 1, wherein the plurality of user discernable indicators comprises a highlighted icon displayed on a computing device.

7. (previously presented) A method, comprising:

defining a set of rules to detect inappropriate communication activity on a computer or network;

separating the rules in the set into a plurality of classes;

associating each of the plurality of classes with a different one of a plurality of user discernable indicators;

examining data traffic to determine whether at least one of the rules has been violated; and

in the case that at least one of the rules of a first one of said plurality of classes has been violated, filtering said data traffic violating the at least one of the rules of the first one of said plurality of classes, providing a user discernable notification of said violation by triggering a respective one of the plurality of user discernable indicators associated with the first one of said plurality of classes, and wherein the rules in the set are prioritized such that each of the plurality of classes represents a respective different one of a plurality of priority levels.

8. (original) The method of claim 7, further comprising:

determining if a first threshold level of rule violation has been exceeded prior to filtering said data traffic.

9. (original) The method of claim 7, further comprising:

determining if a first threshold level of rule violation has been exceeded prior to triggering the user discernable indicator.

10-15. (cancelled)

16. (previously presented) A cable modem, comprising:

downstream processing circuitry;

upstream processing circuitry;

a controller in communication with said downstream circuits, upstream circuitry, and a memory;

a firewall program including a set of rules for identifying packets associated with inappropriate activity, the rules being separated into a plurality of classes, said firewall program being resident in said memory and executable by said controller to cause examining data of packets from said downstream and upstream circuitry; and

a plurality of user discernable indicators, wherein each of the plurality of user discernable indicators is associated with a different one of the plurality of classes and wherein a respective one of said plurality of user discernable indicators is triggered if one or more of the rules corresponding to one of said plurality of classes associated with the respective one of said plurality of user discernable indicators is violated, and wherein the rules in the set are prioritized such that each of the plurality of classes represents a respective different one of a plurality of priority levels.

17. (cancelled)

18. (previously presented) The cable modem of claim 16, wherein said plurality of user discernable indicators comprises a first LED for signifying a filtering event and a second LED for signifying filtering data packets deemed pernicious in said set of rules.

19. (previously presented) The apparatus of claim 16, wherein said plurality of user discernable indicators comprises a highlighted icon displayed on a computer device.

20. (previously presented) The apparatus of claim 1, wherein the firewall filters any of the packets that violate the one or more rules irrespective of a number of the packets that violate the one or more rules, but only triggers the respective one of the plurality of user discernable indicators when the number of the packets that violate the one or more rules exceeds a pre-specified threshold.

21. (previously presented) The method of claim 7, wherein the data traffic includes a number of packets that violate the at least one of the rules of the first one of the plurality of classes, and wherein the method filters the packets that violate the at least one of the rules of the first one of the plurality of classes, irrespective of the number of packets that violate the one or more rules, but only triggers the respective one of the plurality of user discernable indicators when the number of packets that violate the at least one of the rules of the first one of the plurality of classes exceeds a pre-specified threshold.

22. (previously presented) The apparatus of claim 16, wherein the firewall program is executable by said controller to cause filtering of any of the packets that violate the one or more rules irrespective of a number of the packets that violate the one or more rules, but wherein the respective one of the plurality of user discernable indicators is triggered only when the number of packets that violate the one or more rules exceeds a pre-specified threshold.

23. (previously presented) The apparatus of claim 1, wherein each of the plurality of user discernable indicators except a particular one is associated with the respective different one of the plurality of classes, the particular one of the plurality of user discernable indicators being associated with an affirmative status that filtering is being contemporaneously performed for any of the packets that violate the one or more rules, and wherein the method further comprises filtering any of the packets that violate the one or more rules, and wherein the particular one of the plurality of user discernable indicators is concurrently triggered, along with the respective one of the plurality of user discernable indicators, to indicate that the filtering is being contemporaneously performed, only when a number of the packets that violate the one or more rules exceeds a pre-specified threshold.

24. (previously presented) The apparatus of claim 23, wherein only the particular one of the plurality of user discernable indicators is triggered if the one or more of the rules is violated, the filtering is performed by the firewall program, and the number of the packets that violate the one or more rules does not exceed the pre-specified threshold.

25. (previously presented) The apparatus of claim 23, wherein only the respective one of the plurality of user discernable indicators is triggered if the one or more of the rules is violated, the filtering is performed by the firewall program, and the number of the packets that violate the one or more rules does not exceed the pre-specified threshold.

26. (previously presented) The apparatus of claim 1, wherein whether the respective one of the plurality of user discernable indicators is triggered or not is based on which of the plurality of priority levels is involved with respect to a corresponding rule violation.

27. (previously presented) The method of claim 7, wherein each of the plurality of user discernable indicators except a particular one is associated with the different one of the plurality of classes, and the method further comprises:

associating the particular one of the plurality of user discernable indicators with an affirmative status that filtering is being contemporaneously performed for any of the packets that violate at least one of the rules; and

in the case of the rule of at least a first class from among the plurality of classes being violated and a number of packets violating the rule of at least the first class exceeding a pre-specified threshold, providing a user discernable notification of the filtering being contemporaneously performed by triggering, concurrently with the triggering of the respective one of the plurality of user discernable indicators, the particular one of the plurality of user discernable indicators associated with the affirmative status that the filtering is being contemporaneously performed.

28. (previously presented) The method of claim 27, wherein in the case of the rule of at least the first class being violated and the number of packets violating the rule of at least the first class not exceeding the pre-specified threshold, only providing the user discernable notification of the filtering without providing the user discernable notification of the violation.

29. (previously presented) The method of claim 27, wherein in the case of the rule of at least the first class being violated and the number of packets violating the rule of at least the first class not exceeding the pre-specified threshold, only providing the user discernable notification of the violation without providing the user discernable notification of the filtering.

30. (previously presented) The method of claim 7, wherein whether the respective one of the plurality of user discernable indicators is triggered or not is based on which of the plurality of priority levels is involved with respect to a corresponding rule violation.

31. (previously presented) The apparatus of claim 16, wherein the firewall program is executable by said controller to cause filtering any of the packets that at least one of the rules, and wherein each of the plurality of user discernable indicators other than a particular one is respectively associated with the different ones of the plurality of classes, the particular one of the plurality of user discernable indicators being associated with an affirmative status that filtering is being contemporaneously performed, and wherein the particular one of the plurality of user discernable indicators is triggered, concurrently with the triggering of the respective one of the plurality of user discernable indicators, if the one or more of the rules is violated, the filtering is performed by the firewall program, and a number of the packets that violate the one or more rules exceeds a pre-specified threshold.

32. (previously presented) The apparatus of claim 31, wherein only the particular one of

the plurality of user discernable indicators is triggered if the one or more of the rules is violated, the filtering is performed by the firewall program, and the number of the packets that violate the one or more rules does not exceed a pre-specified threshold.

33. (previously presented) The apparatus of claim 31, wherein only the respective one of the plurality of user discernable indicators is triggered if the one or more of the rules is violated, the filtering is performed by the firewall program, and the number of the packets that violate the one or more rules does not exceed a pre-specified threshold.

34. (previously presented) The apparatus of claim 16, wherein whether the respective one of the plurality of user discernable indicators is triggered or not is based on which of the plurality of priority levels is involved with respect to a corresponding rule violation.

35. (previously presented) The apparatus of claim 1, where each of the plurality of classes uses a different one of a plurality of thresholds with respect to how many violating ones of the packets must be detected before filtering is commenced, the plurality of thresholds being end-user settable.

9. RELATED EVIDENCE APPENDIX

None.

10. RELATED PROCEEDINGS APPENDIX

None